Proceedings of AISB 2004 Symposium on The Immune System and Cognition (ImmCog-2004), Leeds, UK, March 2004, pp. 45-46.

An Artificial Immune System for Misbehavior Detection in Mobile Ad Hoc Networks with both Innate, Adaptive Subsystems and with Danger Signal

(work in progress)

Slaviša Sarafijanović and Jean-Yves Le Boudec
{slavisa.sarafijanovic, jean-yves.leboudec}@epfl.ch
EPFL/IC/ISC/LCA,
CH-1015 Lausanne, Switzerland

***Index Terms*— Mobile, ad-hoc, misbehavior, detection, artificial, immune, clonal selection, learning, adaptive, cognitive.**

I. Extended Abstract

A. Problem Statement and Related Work: Detecting Misbehaving Nodes in DSR

The successful operation of a mobile ad hoc network depends on cooperation of the nodes in providing services to each other. Nodes act both as terminals and information relays, and participate in a common routing protocol, such as Dynamic Source Routing (DSR) [13]. The network is vulnerable due to faulty or malicious nodes. Misbehavior detection systems aim at removing this vulnerability [1], [2], [3], [4], [6], [7].

Our approach for misbehavior detection in DSR is to use an Artificial Immune System (AIS) [14], [15]. The system is inspired by the natural immune system of vertebrates [10]. The main task of the natural immune system (the IS) is to protect the human body against microorganism invaders and some malfunctioning own cells, while being tolerant to normal own cells, self cells. To accomplish this task, the IS has developed some detection and reaction mechanisms and procedures, which may be useful for solving analogous problems in building an AIS.

The work presented here is a continuation of our previous work [6], [7]. In the previous work we proposed a solution for mapping some basic parts of the IS to our AIS: representation, matching, and negative and clonal selection. We implemented and validated the solution in the Glomosim simulator [11]. The system had a separate preliminary phase for collecting self-behavior examples. This phase had to be run in a protected environment, when there is no misbehavior of the nodes. It is very hard to provide such conditions in a real network.

In this work we give three main improvements for our AIS. First, we propose a solution that doesn't require a preliminary learning phase in the protected environment (the environment without misbehavior). The solution uses analogy with the IS danger signal [8], [9]. Second, we add the innate part of the AIS, which provides fast detection of misbehavior patterns that are known in advance and for which specific detection mechanisms are designed. For the innate part we adopt solution given in [3]. Third, we introduce information exchange between the nodes, which is analogous to the use of cytokines in the IS; for the information exchange we use the robust reputation scheme proposed in [2]. In our previous work, there was one immune system per network node; with this third improvement, there is one global immune system, distributed across all nodes.

The authors are with EPFL, Lausanne, Switzerland. The work presented in this paper was supported (in part) by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center supported by the Swiss National Science Foundation, under the grant number 5005-67322.

B. Learning Changing Self in an Unprotected Environment. Use of Danger Signal.

The main difficulties for providing self-tolerance in our case are caused by the fact that the system to be protected (mobile ad hoc network running DSR) changes over time. This is because of mobility, changes in nodes' traffic and software updates. The AIS need to learn to differentiate between **new** normal behavior and misbehavior. Our solution for learning changing self, that works well if started in possibly unprotected environment (that may contain misbehaving nodes) is given on Figure 1.

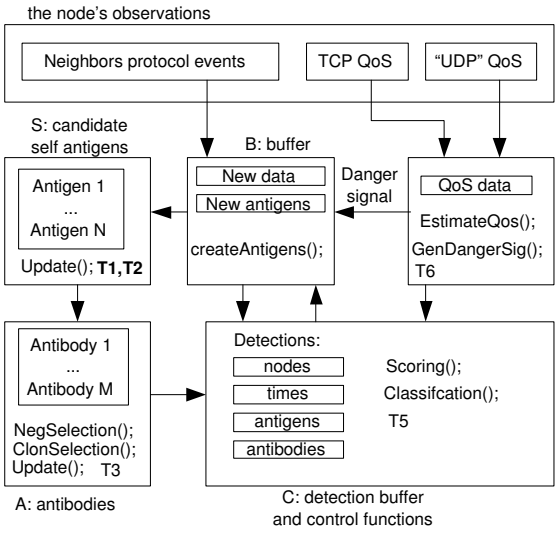

Fig. 1. Learning self antigens in an unprotected environment. The scheme works even if misbehavior is present during both initial and normal operation phase.

The main idea is to use the quality of service (QoS) obtained by a node when is communicating over some neighbors,

and correlate it with matching results on the antigens that are describing observed behavior for that neighbors in the near past. QoS measures that we use are throughput of TCP connections and response time of applications which use UDP, as compared to their estimated normal values. An antigen is created from the data collected during an interval Δt. For more details on representation, matching, and classification see [6], [7].

Here is how the scheme shown in Figure 1 works. Initially, all collected self antigens become 'candidate self antigens', until S becomes full. Then the initial set of antibodies is created. Subsequently collected antigens are buffered in B. They will be checked for matching, and detection results will be temporally stored in C, for both antibodies and antigens. The corresponding node and the time of the detection are also temporarily stored in C. The storing time is determined by T_5 (T_i are system constants). T_5 controls how much time on average are detection results collected for some node, before it is classified as misbehaving.

If there is no matching between the current set of antibodies and an antigen that is collected by the node for one of its neighbors, if no bad QoS is experienced by the node over that neighbor, and if no bad QoS is reported in a sufficient amount for that neighbor by others, in the near past, the antigen will be used for the updating S. The minimal update interval is determined by the constant ΔT; it controls the maximum speed of change of the protected system that may be followed by the AIS, when QoS is good.

The antigens that belong to a node, for which there is enough evidence that it misbehaves, will not be used for updating S. The evidence is calculated from own detections and experienced QoS, and the detections and QoS reported by neighbors. By this distributed filtering, we achieve that S is updated with self antigens. Updates by nonself antigens happen quite rarely, because we use additional latency T_1 (in addition to T_5) in updating the set of self antigens; this time constant is larger than the time needed by the system to detect the node which generated it, unless we have persistently good QoS in the near past (T_4). A nonself antigen that passes this barriers and deletes antibodies reactive to it will also be detected and eliminated from S, but only by the correlating it to bad QoS, and after a longer time, and then again the antibodies will be created that contain knowledge of this antigen and speeds up the detection.

There are two types of antibodies: normal, with T_3 half life time, and memory, that has an infinite life time. Normal antibodies die if they are not useful in detection for some time. Our AIS deletes self-reactive memory antibodies, unlike in the IS case. If a memory antibody consistently matches antigens collected during good QoS in the neighborhood, it will be deleted. In this way, we solve the problem of chronical auto-immunity that is usually caused by mimicry between self and experienced nonself antigens. Such a solution is not used by the IS, because of antigen presenting cells APC and lymphocyte trafficking constraints [10].

C. Using both the innate and the adaptive part

The innate part of the natiral IS has fast detection and reaction against some pathogens with known nonself patterns on their surface. For some misbehavior types, the innate part may detect that an attack is maybe going on, but it has no appropriate detection and reaction to resolve the problem. In both cases it signals to the adaptive part, mobilizing more resources of the adaptive part. This signaling is important because some of attacks are not solved by the innate part, but by the adaptive part or by a cooperative effort.

The part of our solution described in Section I-B is the adaptive part of our AIS. We add the innate part by coding mechanisms that directly detect events which refer to misbehavior or possibility of misbehavior. Such events are non-forwarding route request or data packets, and some unallowed changes in protocol fields in relayed packets. Our innate system influences the adaptive system in that the adaptive systems reacts more quickly when there is evidence that the innate part has detected anomalies. This is analogous to battlefield cytokines in the natural IS.

D. Distributed AIS. Cooperation of nodes. Information exchange

Detection, classification and QoS information are exchanged between the nodes adopting the reputation system proposed in [2], [3]. This provides faster gathering the evidence needed for safe classification of nodes as misbehaving, and reaction against them. It also changes our analogy to the natural IS in that the body to be protected is now the entire network instead of nodes in isolation.

E. Model Validation

We implement and validate our model in the ns-2 simulator [12]. We show improvements over previous work in time to response, ability to detect new attacks, and false positive ratios.

REFERENCES

[1] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of MOBICOM 2000*, pages 255–265, 2000.

[2] S. Buchegger and J.-Y. Le Boudec. A Robust Reputation System for Mobile ad hoc Networks. Technical Report IC/2003/50, EPFL-DI-ICA, Lausanne, Switzerland, July 2003.

[3] S. Buchegger and J.-Y. Le Boudec. Performance Analysis of the CONFIDANT protocol: Cooperation of nodes - Fairness In Distributed Ad-Hoc Networks. In *Proceedings of IEEE/ACM Symposium on Mobile Ad-Hoc Networking and Computing (MobiHOC)*, Lausanne, CH, June 2002. IEEE.

[4] S. Buchegger and J.-Y. Le Boudec. The Effect of Rumor Spreading in Reputation Systems for Mobile Ad-hoc Networks. In *Proceedings of WiOpt '03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks"*, Sophia-Antipolis, France, March 2003.

[5] S. Buchegger, Cedric Tissieres, J. Y. Le Boudec "A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks - How Much Can Watchdogs Really Do?" Technical report No. IC/2003/72, November 2003.

[6] J. Y. Le Boudec and S. Sarafijanovic. An Artificial Immune System Approach to Misbehavior Detection in Mobile Ad-Hoc Networks. Proceedings of Bio-ADIT 2004, Lausanne, Switzerland, January 2004, pp..

[7] S. Sarafijanovic and J. Y. Le Boudec. An Artificial Immune System Approach with Secondary Response for Misbehavior Detection in Mobile Ad-Hoc Networks. TechReport IC/2003/65, EPFL-DI-ICA, Lausanne, Switzerland, November 2003.

[8] P. Matzinger. Tolerance, Danger and the Extended Family. *Annual Review of Immunology*, 12:991-1045, 1994.

[9] P. Matzinger. The Danger Model in it's Historical Contex. *Scandinavian Journal of Immunology*, 54:4-9, 2001.

[10] L.M. Sompayrac. How the Immune System Works, 2nd Edition. Blackwell Publishing, 2003.

[11] Xiang Zeng, Rajive Bagrodia, and Mario Gerla. Glomosim: A library for parallel simulation of large scale wireless networks. *Proceedings of the 12th workshop on Parallel and Distributed Simulations-PDAS'98*, May 26-29, in Banff, Alberta, Canada, 1998.

[12] The network simulator ns-2, http://www.isi.edu/nsnam/ns/.

[13] D.B. Johnson and D.A. Maltz. The dynamic source routing protocol for mobile ad hoc networks. *Internet draft, Mobile Ad Hoc Network (MANET) Working Group*, IETF, February 2003.

[14] De Castro, L. N. and Von Zuben, F. J. (1999), "Artificial Immune Systems: Part I Basic Theory and Applications", Technical Report RT DCA 01/99.

[15] Leandro N. de Castro and Jonathan Timmis, "Artificial Immune Systems: A New Computational Intelligence Approach" , Springer Verlag, Berlin, 2002.